

The Wayback Machine - https://web.archive.org/web/20220426143718/https://cc.bingj.com/cache.aspx?q=%22Mitel+Voice+Over+IP+Servers+Disclose+...
Hai raggiunto la pagina nella memoria cache per <https://securitytracker.com/id/1007428>

Di seguito è disponibile lo snapshot della pagina Web alla data **19/06/2021** (l'ultima volta che è stata visitata dal nostro crawler). Questa è la versione della pagina utilizzata per la classificazione dei risultati della ricerca. La pagina potrebbe essere stata modificata dall'ultima volta che è stata memorizzata nella cache. Per verificare le eventuali modifiche (senza evidenziazioni), [go vai alla pagina corrente](#).

Hai cercato: "**Mitel Voice Over IP Servers Disclose Calling Data to Remote Users**" Le parole corrispondenti della pagina sottostante sono state evidenziate.

Bing non è responsabile del contenuto di questa pagina.



[Home](#) | [View Topics](#) | [Search](#) | [Contact Us](#) |

SecurityTracker
Archives

Category: [Application \(VoIP\)](#) > [Mitel VoIP](#)

Vendors: [Mitel Networks](#)

(Vendor Confirms and Clarifies) Re: Mitel Voice Over IP Servers Disclose Calling Data to Remote Users

SecurityTracker Alert ID: 1007428

SecurityTracker URL: <http://securitytracker.com/id/1007428>

CVE Reference: [GENERIC-MAP-NOMATCH](#) (Links to External Site)

Date: Aug 7 2003

Impact: [Disclosure of system information](#), [Disclosure of user information](#)

Vendor Confirmed: Yes

Version(s): 3100 ICP

Description: A vulnerability was reported in Mitel's voice over IP (VoIP) systems. A remote user can obtain information about calls made via the system.

Acme reported that a remote user can connect to the target server's telnet port when a call is in place to gain information about the call in progress.

A remote user can attempt to login several times without success. However, when an outside call arrives, the system will reportedly display information about the call. Information provided includes the type of service, the extension number, and other call activity parameters,

according to the report.

An exploit transcript is provided in the original advisory. The original advisory is available (in Italian language) at:

<http://olografix.org/acme/mitel.txt>

Impact: A remote user on the internal network can obtain information about telephone calls on the system.

Solution: The vendor has confirmed the flaw and is preparing a fix for an upcoming release.

The vendor has also clarified that a user must be on the internal network to connect to the device.

Vendor URL: www.mitel.com/ (Links to External Site)

Cause: [Access control error](#), [State error](#)

Message History: This archive entry is a follow-up to the message listed below.

Jul 28 2003 [Mitel Voice Over IP Servers Disclose Calling Data to Remote Users](#)

 **Source Message Contents**

Subject: (Mitel Response) [Mitel Voice Over IP Servers Disclose Calling Data to Remote Users](#)

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Mitel Networks has confirmed that this vulnerability only affects the 3100 ICP, one of our range of VoIP systems. The vulnerability is not remotely exploitable as access to the local (internal) network of the 3100 ICP is required. When a user attempts to login via telnet, they will see any SMDR records generated by the system during the time they are waiting for a login.

It is important to emphasize again that a user must be on the local LAN to which the 3100 ICP is connected in order to exploit this vulnerability. It is NOT possible to access this information from outside of the local network.

A solution to this vulnerability will be provided in an upcoming release of the 3100 ICP.

Please send any concerns about this issue, or any other security issues, to:

security@mitel.com

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.2 (MingW32) - WinPT 0.7.96rc1

iD8DBQE/KrSTQiNa0wAEkqYRApNUAJ9n3vBYZ4B4WLaz76pSN/gmBSJL6gCcDvom

lad6DzEYroG0xggrFJnkeFQ=

=QPqQ

-----END PGP SIGNATURE-----

[Go to the Top of This Security Tracker Archive Page](#)

[Home](#) | [View Topics](#) | [Search](#) | [Contact Us](#)

This web site uses cookies for web analytics. [Learn More](#)

Copyright 2021, SecurityGlobal.net LLC